

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-274006

(43)Date of publication of application : 26.09.2003

(51)Int.Cl.

H04M 1/667
 G06F 15/00
 G06T 7/00
 H04M 1/02
 H04M 1/21
 H04Q 7/38

(21)Application number : 2002-074331

(71)Applicant : NEC COMMUN SYST LTD

(22)Date of filing : 18.03.2002

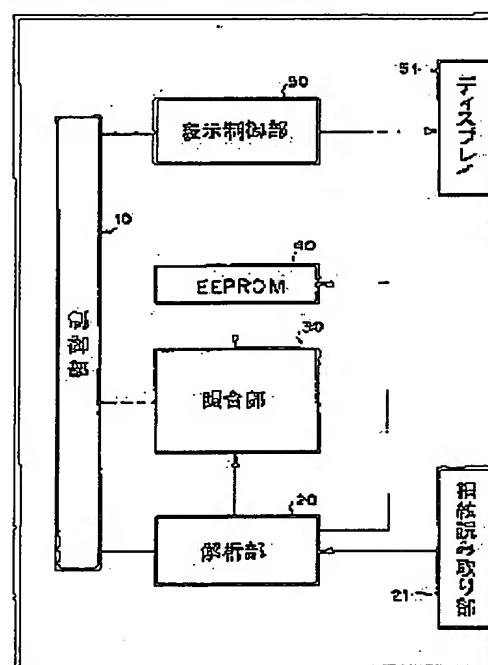
(72)Inventor : SAKAMOTO MASATAKA

(54) MOBILE PHONE WITH FINGERPRINT AUTHENTICATION FUNCTION AND PERSON AUTHENTICATING METHOD THEREOF

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a mobile phone with a fingerprint authentication function whereby a fingerprint is used for authentication of a person to enhance security.

SOLUTION: When a user places its finger to a fingerprint read section 21 after a display apparatus 51 displays start of registration, reading of fingerprint data is started and the fingerprint data are converted into feature data such as a feature point and relation. A nonvolatile memory 40 stores the feature data, and registration processing is finished. When the user places its finger to the fingerprint read section 21 during operation of the fingerprint authentication function, the fingerprint data are converted into feature data such as a feature point and relation. Collation data are extracted from the nonvolatile memory 40 and cross-referenced with the extracted feature data for calculation of a score. Coincidence/dissidence is discriminated depending on the magnitude relation between the score and a threshold value. When the discrimination indicates coincidence, the succeeding operation is executed and when dissidence is discriminated, power is interrupted to inhibit further operations.



LEGAL STATUS

[Date of request for examination]

10.02.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-274006

(P2003-274006A)

(43) 公開日 平成15年9月26日 (2003.9.26)

(51) Int.Cl. ⁷	識別記号	F I	テ-マ-ト ⁷ (参考)
H 0 4 M 1/667		H 0 4 M 1/667	5 B 0 4 3
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 F 5 B 0 8 5
G 0 6 T 7/00	5 3 0	G 0 6 T 7/00	5 3 0 5 K 0 2 3
H 0 4 M 1/02		H 0 4 M 1/02	C 5 K 0 2 7
1/21		1/21	L 5 K 0 6 7
審査請求 有 請求項の数 6 O L (全 5 頁) 最終頁に続く			

(21) 出願番号 特願2002-74331(P2002-74331)

(22) 出願日 平成14年3月18日 (2002.3.18)

(71) 出願人 000232254

日本電気通信システム株式会社

東京都港区三田1丁目4番28号

(72) 発明者 坂本 昌隆

神奈川県川崎市中原区小杉町一丁目403番

地 日本電気テレコムシステム株式会社内

(74) 代理人 100065385

弁理士 山下 穰平

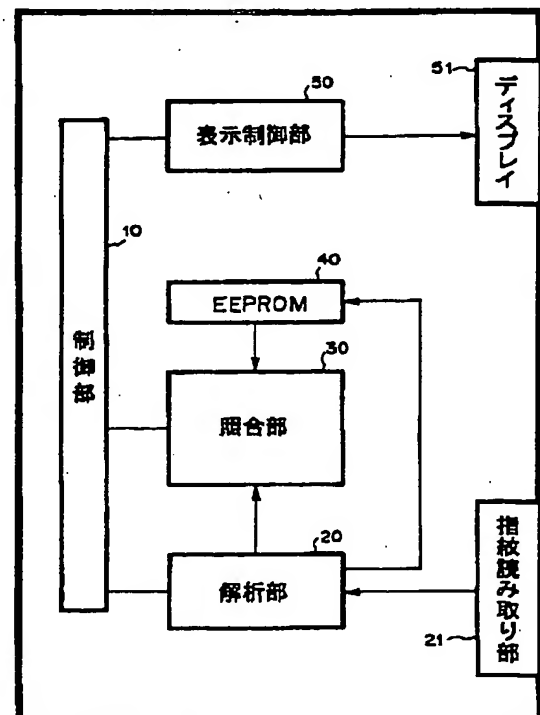
最終頁に続く

(54) 【発明の名称】 指紋認証機能を有する携帯電話機及びその個人認証方法

(57) 【要約】

【課題】 指紋を個人認証に利用してセキュリティを高めた指紋認証機能を有する携帯電話機を提供する。

【解決手段】 ディスプレイ 51 に登録開始表示後、ユーザが指紋読み取り部 21 に指を置くと、指紋データの読み込みが開始され、指紋データは、特徴点、リレーション等の特徴データに変換される。この特徴データを不揮発メモリ 40 に格納し、登録処理は終了となる。指紋認証機能動作中に指紋読み取り部 21 に指を置くと、指紋データの読み込みが開始され、指紋データは、特徴点、リレーション等の特徴データに変換される。不揮発メモリ 40 より照合データを取り出し、抽出した特徴データとの対応をとりスコアを計算する。このスコアと閾値との大小により一致、不一致を判定する。一致であれば以降の動作を実施し、不一致であれば電源 OFF にして、これ以上操作できないようにする。



(2)

【特許請求の範囲】

【請求項1】 使用者の個人認証機能を有する携帯電話機であって、

電源投入後、指紋認証データの有無を判定して、指紋認証データが登録されていない場合、読み取った指紋の特徴データを前記指紋認証データとして登録する認証データ登録処理手段と、

前記指紋認証データが登録済みの場合、読み取った指紋の特徴データと登録済みの指紋認証データとの照合を行う指紋認証処理手段と、

照合結果が一致の場合、立ち上げ処理をして、待ち受け動作に移行する手段と、

照合結果が不一致の場合、電源をオフにして、以降の操作をできないようにする手段とを備えることを特徴とする指紋認証機能を有する携帯電話機。

【請求項2】 前記指紋認証データとして、指紋の特徴点とリレーションの情報をを用いることを特徴とする請求項1記載の指紋認証機能を有する携帯電話機。

【請求項3】 待ち受け動作時の個人認証を必要とする処理において、

読み取った指紋の特徴データと前記指紋認証データとの照合を行う指紋認証処理を行い、

照合結果が一致の場合、前記個人認証を必要とする処理に移行し、照合結果が不一致の場合、電源をオフにして、以降の操作をできないようにすることを特徴とする請求項1又は2記載の指紋認証機能を有する携帯電話機。

【請求項4】 指紋認証機能を有する携帯電話機の個人認証方法であって、

電源投入後、指紋認証データの有無を判定して、指紋認証データが登録されていない場合、読み取った指紋の特徴データを前記指紋認証データとして登録処理を行い、前記指紋認証データが登録済みの場合、読み取った指紋の特徴データと登録済みの指紋認証データとの照合をする認証処理を行い、

照合結果が一致の場合、立ち上げ処理をして、待ち受け動作に移行し、

照合結果が不一致の場合、電源をオフにして、以降の操作をできないようにすることを特徴とする携帯電話機の個人認証方法。

【請求項5】 前記指紋認証データとして、指紋の特徴点とリレーションの情報をを用いることを特徴とする請求項4記載の携帯電話機の個人認証方法。

【請求項6】 待ち受け動作時の個人認証を必要とする処理において、

読み取った指紋の特徴データと前記指紋認証データとの照合を行う指紋認証処理を行い、

照合結果が一致の場合、前記個人認証を必要とする処理に移行し、照合結果が不一致の場合、電源をオフにして、以降の操作をできないようにすることを特徴とする

請求項4又は5記載の携帯電話機の個人認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、指紋による個人認証機能を有する携帯電話機に関する。

【0002】

【従来の技術】従来、携帯電話機のセキュリティシステムとして、パスワードを入力して登録された個人を認証するパスワード方式がある。

10 【0003】また、特開平11-262059号公報では、携帯端末の個人識別情報としてパスワードの替わりに指紋データを用いる移動通信用携帯端末における個人識別方法が開示されている。

【0004】

【発明が解決しようとする課題】しかしながら、パスワード方式はパスワードを解析されて悪用されるおそれがある。また、データに関するセキュリティ等は、暗号化等によって強化されているが、携帯電話機自体のセキュリティはパスワード等によるもので、強化されているとは言えない状況である。

20 【0005】また、従来の指紋データを用いる携帯端末の個人識別方法は、音声通話を前提として、携帯端末から発信するときに、発信ボタンを押下する際に読み取った使用者の指紋データと、あらかじめROMに記憶された指紋データとを照合して発信の可否を判断するので、データ通信によるメールの送受信を行う近年の携帯電話機では、受信したメールを他の人に見られてしまう危険性がある。

30 【0006】そこで本発明は、各個人に固有の情報である指紋を個人認証に利用してセキュリティを高めた指紋認証機能を有する携帯電話機及びその個人認証方法を提供することを目的とする。

【0007】

40 【課題を解決するための手段】上述の課題を解決するため、本発明は、使用者の個人認証機能を有する携帯電話機であって、電源投入後、指紋認証データの有無を判定して、指紋認証データが登録されていない場合、読み取った指紋の特徴データを前記指紋認証データとして登録する認証データ登録処理手段と、前記指紋認証データが登録済みの場合、読み取った指紋の特徴データと登録済みの指紋認証データとの照合を行う指紋認証処理手段と、照合結果が一致の場合、立ち上げ処理をして、待ち受け動作に移行する手段と、照合結果が不一致の場合、電源をオフにして、以降の操作をできないようにする手段とを備え、前記指紋認証データとして、指紋の特徴点とリレーションの情報をを用いることを特徴とする。

50 【0008】なお、指紋認証は特徴点とリレーション方式のアルゴリズム（特許1289457号（特公昭60-12674号）、特許1468842号（特公昭63-13226号））を使用する。

(3)

3

【0009】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して説明する。

【0010】一般に、指紋データにより個人を特定する場合、以下の照合方法がある。

「1対1照合」：登録されている多数の指紋の中から

「IDなどの情報」により指紋を特定した上で入力された指紋と照合を行い、個人を特定する方法。

「1対N照合」：登録されている全ての指紋の中から指紋データのみで入力された指紋と照合を行い、一致する指紋を探し出す方法。

【0011】本発明では、入力された指紋データのみで一致する指紋を探し出す「1対N照合」を行う。この

「1対N照合」を実現するには高い照合精度を必要とする。すなわち、他人許容率（登録されていない指紋を登録されている指紋と誤って認識してしまう率）を小さくすると共に本人拒否率（登録されている指紋を登録されていない指紋と誤って認識してしまう率）を小さくする必要がある。このため、指紋照合に特徴点及びリレーションの情報をを用いることで、他人許容率小さくすると共に本人拒否率を小さくして、安全性と利便性を兼ね備えている。

【0012】この特徴点とリレーションについて、図1を参照して説明する。図1(a)に示すように、指紋の模様を形成する盛り上がっているところを「隆線」と呼ぶ。この隆線には、切れている部分と分岐している部分がある。切れている部分を「端点」、分岐しているところを「分岐点」と呼ぶ。この「端点」と「分岐点」を合わせて「特徴点」と呼んでいる。通常の指紋では、指紋の中心部分の特徴点は、約50である。この特徴点から得られる「位置」と「方向」を特徴点の基本情報として扱う。

【0013】しかし、特徴点の位置と方向の情報だけでは、偶然に一致する可能性がある。そこでリレーションと呼ばれる情報を付加する。図1(b)に示すように、「リレーション」とは、特徴点と他の特徴点との間を横切る「隆線」の数の情報で、特徴点の情報に付加することによって、特徴点の位置と方向の情報だけを用いた場合に比べ、指紋照合精度が格段に向上する。

【0014】図2は、本発明による携帯電話機(PDC(Personal Digital Cellular)、W-CDMA(Wideband Code Division Multiple Access)、PHS(Personal Handyphone System)等による方式を含む)の指紋認証処理部の構成を示す。まず個人データの登録処理を説明する。制御部10より解析部20へ個人データ登録指示を送ると共に、表示制御部50へ登録開始表示の指示を送る。ディスプレイ51に登録開始が表示されるとユーザは、指紋読み取り部21へ指を置く。指紋データの読み込みが開始され、指紋データは解析部20にて、特徴点、リレーション等の特徴データに変換される。この特

4

徴データをEEPROM等の不揮発メモリ40に格納し、制御部10へ登録完了を通知する。制御部10は表示制御部50へ登録完了表示の指示を送る。ディスプレイ51に登録完了が表示され登録処理は終了となる。

【0015】続けて、指紋認証処理を説明する。指紋認証機能動作中に指紋読み取り部21へ指を置くと、指紋データの読み込みが開始される。指紋データは解析部20にて、特徴点、リレーション等の特徴データに変換される。続いて、照合部30では、不揮発メモリ40より照合データを取り出し、抽出した特徴データとの対応をとりスコアを計算する。このスコアと閾値との大小により一致、不一致を判定する。一致であれば以降の動作を実施し、不一致であれば電源OFF等にして、これ以上操作できないようにする。

【0016】次に、図3以降のフローチャートを参照して本発明による携帯電話機全体の動作について説明する。まず、指紋による個人認証用のデータを登録する必要があるが、これはユーザが携帯電話機購入後、初めての電源投入時に行う。電源投入後(S10)、認証データが無い場合(S20)、制御部10から表示制御部50へ認証データ登録開始表示を指示し(S30)、図4に示すフローチャートの認証データ登録処理に移行する。認証データ登録処理ではまず、特徴抽出が行われる(S31)。図5はその特徴抽出処理のフローチャートであり、解析部20にて、指紋読み取り部21より読み込んだ(S311)指紋データから特徴点を抽出し(S312)、その後にリレーションの抽出を行う(S313)。特徴抽出が完了したら、データをEEPROM40へ書き込む(S32)。制御部10は、認証データ登録完了の表示を表示制御部50へ指示する。

【0017】認証データの登録が完了したら(または既に認証データが登録されている場合)、制御部10は、照合部30に認証処理を指示すると共に、表示制御部50へ認証開始表示を指示する(S40)。すると、図6に示すフローチャートの認証処理に移行する。照合部30は解析部20へ特徴抽出を指示する。解析部20は、認証データ登録と同様に特徴抽出を行い(S41)、照合部30へ特徴抽出データを渡す。特徴抽出データを受け取った照合部30は、EEPROM40から照合データを読み出し(S42)、照合を行いスコアを算出する(S43)。スコアと決められた閾値との大小により照合データと一致したかどうか判断し(S44)、その結果を制御部10へ渡す。制御部10は照合結果が不一致の場合、表示制御部50へ照合NGの表示を指示し、電源OFFを行い(S45)、以降の操作をできないようにする。照合結果が一致の場合は、表示制御部50へ照合OKの表示を指示し、立ち上げ処理を行い(S50)、待ち受け処理へと移行する(S60)。

【0018】次に、待ち受け時等の個人認証が必要な処理(積算リセット等、以降は積算リセットで説明)の動

50

(4)

5

作について、図7に示すフローチャートを参照して説明する。なお、積算リセットとは、待ち受け状態から発信したときの通話時間と通話料金を積算して表示する機能であり、これをリセットして0から再スタートするのが積算リセットである。この積算リセットを行うには、誤操作や他人によるいたずらができないように個人認証を必要とする。

【0019】ユーザがメニューから積算リセットを選択すると認証処理を実行する(S70)。制御部10より表示制御部50へ認証開始の表示を指示する。その後の認証処理は前述した図6のフローチャートの認証処理に移行し、解析部20にて特徴抽出を行い(S41)、照合部30にて照合データを読み出し(S42)、照合を行う(S43)。照合結果を受けた制御部10は、照合結果が不一致の場合(S44)、表示制御部50へ照合NGの表示を指示し、電源OFFを行い(S45)、以降の操作をできないようにする。照合結果が一致の場合、表示制御部50へ照合OKの表示を指示し、積算リセット処理を行う(S80)。

【0020】以上の実施形態では、指紋認証に特徴点とリレーション方式のアルゴリズムを使用しているが、他人許容率と本人拒否率とが共に小さく、「1対N照合」を実現する高い照合精度を有する認証方法であれば、他のアルゴリズムでも同様に利用できる。

【0021】

【発明の効果】以上説明したように、本発明による最大の効果は、他人による悪用を防ぐことである。従来のパスワード方式では、解読される可能性がある。さらに昨今の携帯電話機ではデータ通信による金融取引も可能で

6

あり、悪用された場合の被害が大きなものとなることが予想される。しかし、指紋という個人に固有の情報でセキュリティを強化すれば悪用されることがなくなることが期待される。

【0022】また、指紋認証に特徴点とリレーション方式のアルゴリズムを使用することにより、高い照合精度で「1対N照合」を実現することができる。

【図面の簡単な説明】

【図1】(a)は特徴点について、(b)は特徴点とリレーションについての説明図である。

【図2】本発明による携帯電話機の指紋認証処理部の構成図である。

【図3】本発明による携帯電話機全体の動作を説明するフローチャートである。

【図4】認証データ登録処理を説明するフローチャートである。

【図5】特徴抽出処理を説明するフローチャートである。

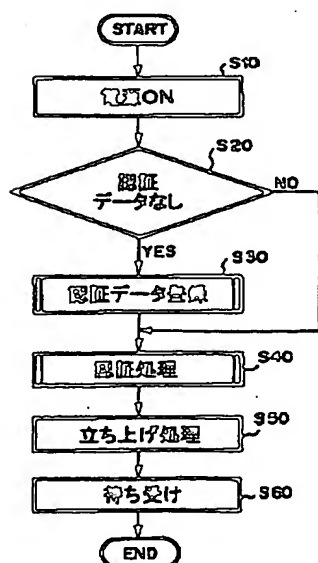
【図6】認証処理を説明するフローチャートである。

【図7】積算リセット処理を説明するフローチャートである。

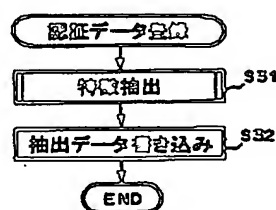
【符号の説明】

- 10 制御部
- 20 解析部
- 21 指紋読み取り部
- 30 照合部
- 40 不揮発メモリ(EEPROM)
- 50 表示制御部
- 51 ディスプレイ

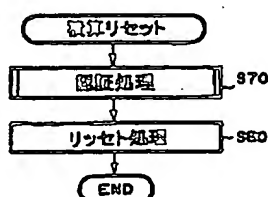
【図3】



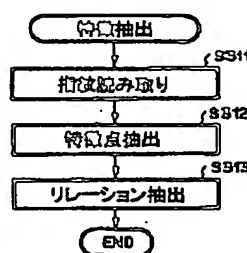
【図4】



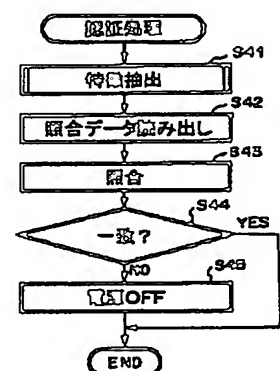
【図7】



【図5】

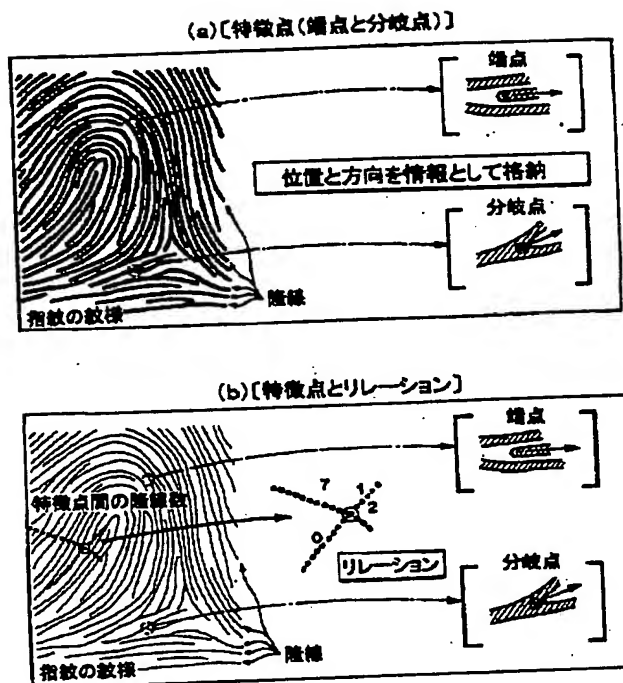


【図6】

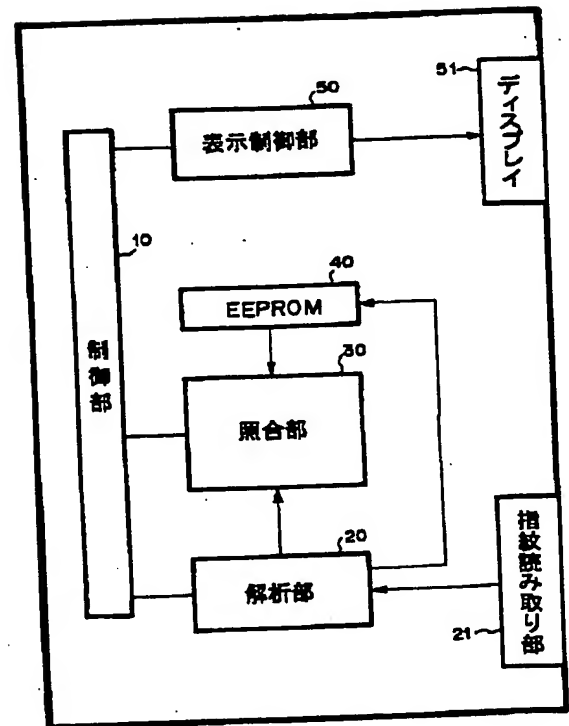


(5)

【図1】



【図2】



フロントページの続き

(51) Int. Cl. 7

識別記号

H 0 4 Q 7/38

F I
H 0 4 B 7/26

テーマコード(参考)

1 0 9 R

F ターム(参考) 5B043 AA09 BA02 EA05 FA03 FA07
GA02
5B085 AA08 AE26 BE03
5K023 AA07 BB21 EE02 LL03 LL06
MM23
5K027 AA11 BB04 CC08 GG02 HH26
5K067 AA32 BB04 DD27 DD52 HH22
HH23 KK05